Cryptologic Almanac 50th Anniversary Series

AFSAM-7

(U) The AFSAM-7 was an important post-World War II milestone in improved communications security. Its importance resided partly in its cryptographic design, but, more importantly, the AFSAM-7 was the product of joint service development of crypto-gear. However, it took more than seven years, with many organizational and technical twists and bureaucratic delays, before it came about.

(U) Before, during, and immediately after World War II, the U.S. Army and Navy took differing cryptologic paths in both communications intelligence and communications security. While they managed limited, on-going cooperation in exploitation of enemy communications, each kept its own systems development private from the other service.

(S) There was one major wartime exception to the services' policy of exclusivity: development of the SIGABA/ECM. In the late 1930s, the Army and Navy cooperated in producing a superior cryptomachine, which kept high-level communications absolutely secure. Called the SIGABA by the Army and ECM(Electric Cipher Machine) by the Navy, it took advantage of the knowledge of both services' top cryptographers -- William F. Friedman and Frank B. Rowlett from the Army and Lieutenant Commander Laurance Safford from the Navy -- and incorporated their best design features. The machine's reliability was rated so highly that it was used through the 1950s -- some of its operating principles were not declassified until the year 2000.

(U) At the tactical level, the services used a variety of crypto-devices for their written messages. Most widespread during the war was the Converter M-209, a relatively lightweight device invented by the Swedish manufacturer Boris Hagelin and licensed for use by American forces. The M-209 was considered satisfactory early in the war, but by 1945 was deemed too inefficient and slow for combat use. Moreover, some cryptographers suspected it might be vulnerable to enemy cryptanalysis.

(S) Therefore, in March 1945 the headquarters of the Army Ground Forces requested a faster, more secure tactical cryptomachine. The requirements called for a device that would provide 10 hours of security after each key change, could encipher or decipher 60 five-letter code groups per minute, and weigh no more than 15 pounds. The requirement also called for simplicity of operation and operability in extremes of climate.

(S) The request for a new machine was approved by the Chief Signal Officer, who passed it to the Signal Security Service (which in a few months would be renamed the Army Security Agency), the Army agency responsible for both communications intelligence and communications security.

(S) As part of this process, the Joint Army-Navy Nomenclature Committee assigned the machine the designation "MX-507." The proposal then went through some weeks of coordination and approval with technical and budget committees. Requirements and names would change several times before the new machine was deployed in actual service.

(S) As the project got started, ASA saw development of the MX-507 as just one phase of a long-range project of on-going research that would enable the service to account for changing requirements and changing technology. The intense codebreaking struggle behind the shooting war had shown America's leadership the criticality of secure communications; new technologies, including nascent computers, necessitated higher investment in research and procurement.

(S) The Army was not alone in seeking a new cipher machine. Near the end of the war, the Navy also was seeking a new cipher device. The Navy wanted a hand-operated cipher machine that incorporated SIGABA/ECM principles, but its primary concern was saving weight.

(S) The Air Force did not yet exist as a separate service in 1945 and 1946, so in January 1946 the Army Air Corps began reviewing requirements for crypto-machines. The AAC had two devices in development, but now saw them as likely interim fixes, until the MX-507 would be available.

(S) ASA's policy leadership decided to pursue an entirely new cryptographic principle for the new device, a concept called "re-entry." It had been discovered in mid-1940 by Albert W. Small and patented a year later. Re-entry, also known as "re-flexing," meant feeding the output of one step of a cryptographic system as input into another step and re-enciphering it.

(U//FOUO) ASA research on the new device proceeded slowly in the autumn of 1945. The few available engineers devoted a considerable part of four months to writing detailed reports of their branch projects undertaken during the war. When research began in earnest, ASA's researchers decided that rotor-based machines were still the best method for providing high-security units.

(S) All U.S. cipher machines were off-line, so the new system would also have to have a printer, as had the SIGABA/ECM. Research into a modified printer for the crypto-device initially did not result in any models, but, as one Army historian dryly noted, "it did

produce extensive paper work." Central to the new device would be a bank of 36-point rotors. The first proposed motion for the MX- 507's rotors was deficient; ASA cryptanalysts found that notch patterns on the rotors could be determined with a "reasonable" amount of effort. Research continued.

~~(S)~~ Over time, the project also encountered delays due to successes in research. For example, studies showed new methods of rotor use. Again, after several dead ends in studying different methods of printing, ASA discovered a way to reduce a tape printer to one quarter its original size, with even greater reduction in the printer's weight. Additional work developed what a later era would call "modules," allowing for rapid maintenance of units in the field. But adapting these innovations to the original design required time.

~~(S)~~ In early August 1947, the commanding officer of ASA sent a letter to the Chief of Naval Communications, asking information on several Navy projects so that the two services could avoid duplication of effort. The Navy responded with the requested information a couple of weeks later, but apparently no further interservice cooperation ensued at this time.

~~(S)~~ The Navy, in fact, was about to let out a contract for what it called a "Portable Cipher Machine" (PCM), a revision of the ECM. The Navy intended the device for "minor war vessels" and shore stations, and submarines or other vessels where compactness was necessary. This device also was to employ seven rotors -- with 26 contact points -- and weigh no more than 20 pounds. Delivery was expected by September 1950.

~~(S)~~ Although basic research in the Army had by this time progressed to a stage where development of the entire machine out of its components was feasible, some in ASA still expressed reservations about the motion of the rotors. First, the mechanical motion was difficult to achieve from an engineering standpoint. And, although cryptanalytic attacks on test material had been unsuccessful, the cryptanalysts warned that more advanced studies might reveal exploitable weaknesses. More studies were called for.

~~(S)~~ At this point, William Friedman, a special consultant at ASA, one of the most senior cryptologists in the U.S. government, and one of several who had developed the SIGABA/ECM, spoke urgently of the need for joint communications capabilities among the services. In a speech to a technical group at ASA in March 1948, Friedman noted that while the Army -- then still including the Air Corps, which was on the verge of becoming a separate service -- had a long-range plan for crypto-research, the Navy did not. Friedman expressed the need for a high-level committee that could make joint communications security a reality. Later that year, Friedman further suggested that civilian agencies ought also to be able to use some military crypto-devices.

~~(S)~~ The military and the cryptologic community were not yet ready for this concept. But

cryptologic cooperation, even consolidation, was an idea whose time had come.

(U) In July 1949, the Armed Forces Security Agency (AFSA) was created as the first central cryptologic organization in the United States. Important reasons for the creation of AFSA were the need for standardization of gear and elimination of duplication of effort among the services. One of AFSA's missions was to determine general policy for the services' cryptographic equipment. Research and development of the Army's new cryptosystem was transferred to AFSA in December. At that time, the nomenclature was changed from MX-507 to AFSAM-7.

(S) Since several cipher machine projects were under way in all three services, discussions were held in January and February 1950 with AFSA cryptographers about consolidating projects or sharing technology. Taking note of how far along each was, in April the director of AFSA decided against consolidating the systems then under development in the Army and Navy.

(S) By late September, after saltwater and heat tests of the rotors, and testing of other components, an engineering model of the AFSAM-7 was demonstrated for representatives of all four services. The machine was deemed satisfactory enough to allow the Army to proceed to build prototype models.

(S) In October 1950, the Army pointed out to AFSA policy- makers that the Army and Navy were each developing incompatible systems. The Army machine involved new technology while the Navy's was merely a modification of the existing SIGABA/ECM. The Army's machine used rotors with 36-contact points; the Navy's rotors had 26 points. The Army proposed a basket of new rotors for the older machine to facilitate interservice communications.

(S) On 20 October, AFSA proposed a joint policy for use of AFSAM-7 and another device under development by ASA. ASA concurred. The Director of Naval Communications put the matter under study.

(S) By mid-November, with Army "life tests" of components successfully completed, a joint panel recommended that the AFSAM-7 be considered ready for procurement. There was, however, lack of unanimity among the services. The Navy objected to the idea, saying it was not clear the machine could meet prescribed specifications; the Navy also announced that its new cipher machine, the PCM, would be available in July 1952. The Marine Corps decided that temperature, absorption, and drop tests indicated the fiberglass carrying case for the AFSAM-7 was not adequate for Corps' use. On the other hand, when the Air Force Security Service finally tested the AFSAM-7 in June 1952, the AFSS stated that it would prove to be an "excellent" machine.

(S) Despite this, DIRAFSA declared the AFSAM-7 ready for procurement on December 8, 1950, and the organization moved to select a contractor for the job. At that time, U.S. cryptosystems used titles derived from the ancient world, so the AFSAM-7 was christened "Pollux." ASA and AFSS indicated each would order limited quantities, hundreds rather than thousands.

(S) While interservice policy was being worked out in the organizational stratosphere, the working levels moved ahead with composing operational and maintenance manuals (which would not be released to the printer until the last possible moment, so that it could incorporate all changes) and keying materials. The first course for Army and Air Force personnel on repair and maintenance of the AFSAM-7 was scheduled for September 1951.

(S) In late January 1951, AFSA's Planning Group requested design of components that would permit intercommunication between users of AFSAM-7 and the major cipher devices of each service. AFSA-31 reported that design tests for intercommunication were under way, and a suitable machine model would be ready by August. A proposed cipher unit to account for the difference in Army and Navy devices was developed by March.

(S) Four prospective contractors submitted bids in early February 1951, and a contract was signed within a few days with the lowest bidder. It called for production of 25,000 units, at a rate of 5,000 per year. Despite this optimistic sign, the contractor subsequently encountered tooling difficulties and material shortages, forcing it to postpone the delivery date to June 1952, and then again to January 1953.

(S) In October 1951, DIRAFSA, Major General Ralph Canine, announced to the three services that AFSAM-7 would have two types of operation. The first, named Adonis, would be used by higher level units; in the second, Pollux, the Army and Air Force would use common rotors for interservice communications. Both services placed conditions on the Pollux option, but eventually adopted it. General Canine, a no-nonsense old-Army officer, helped promote it.

(S) A final production contract was signed on February 9, 1952. In addition to the military services, both the Central Intelligence Agency and the Federal Bureau of Investigation bought units. The AFSAM-7 became an important component of American communications security for years.

(S) Today, it may seem surprising that it took nearly eight years to design and field a new cipher machine, but the delay must be understood in the context of the times.

(S) Before the world war, the importance of cryptography had been recognized, but build-up of the fighting forces took priority. After the war, considerable resources were devoted to cryptology (even as the military itself was downsizing drastically), but cryptologic

technology changed rapidly. Constant discovery of new principles and new applications meant design changes had to be made frequently in machines under development, lest they be obsolete -- and vulnerable -- even before deployment. New concepts also raised serious questions that had to be addressed about the vulnerability of older or traditional cryptographic principles.

(U//~~FOUO~~) Despite the precedent of the Army-Navy development of the SIGABA/ECM on the eve of World War II, the concept of joint cryptologic activities was an unfamiliar -- and not entirely welcome -- idea to the services. They had long been rivals for appropriations and the small pool of talented cryptologists, and wanted to preserve their individual service prerogatives. It took the experience of working together and a powerful figure like General Ralph Canine to bring about meaningful cooperation.

[(U//~~FOUO~~) David A. Hatch, Director, Center for Cryptologic History, 972-2893s, dahatch@nsa]

Horizontal Line

Almanac 50th Anniversary Series

Content Owner: Feedback
Web POC: Feedback

Last Modified: by nsr
Last Reviewed: February 28, 2003
Next Review: 365 days